Passive information gathering

Whois

Find out who is behind the website.

Resolve the DNS

```
 host website.com
nslookup website.com
```

The the IP address and check it with `whois`

```
whois 192.168.1.101
```

Netcraft

Most of the info found on netcraft is not unique. It is basic whois info. But one thing is really good, it lists the different IP-addresses the page has had over the years. This can be a good way to **bypass cloudflare** and other services that hide the real IP. Using netcraft we can find the IP that was in use before they implemented cloudflare.

Another detail that is good to know is the **hosting-company** or **domain-provider**. Those details can be used if we want to try some **social-engineering or spear-phishing attack**.

Netcraft

References

http://www.technicalinfo.net/papers/PassiveInfoPart1.html